UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/099,763	03/15/2002	Dong-Hyang Lee	10969-012-999	4127

20583 7590 04/03/2006

JONES DAY
222 EAST 41ST ST
NEW YORK, NY 10017

EXAMINER	
TOLENTINO, RODERICK	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 04/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/099,763	LEE, DONG-HYANG	
	Examiner	Art Unit	
	Roderick Tolentino	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 January 2006*.

2a)☒ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)☒ Claim(s) *1* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *8/22/2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 – 8 are pending.

Response to Arguments

2. Applicant's arguments directed towards claims 1, 6 and 8, filed 1/20/2006 have been fully considered but they are not persuasive.

3. However, Applicant's arguments with respect to added limitations in claims 1, 6 and 8 have been considered but are moot in view of the new ground(s) of rejection.

Applicant had further argued on pages 6 – 9 that in claims 1 and 6 that Parenty fails to teach sending an encryption method in a non- installed method to a client. Examiner respectfully disagrees in part. Parenty does teach sending an encryption method to a client (Parenty, Fig. 2 Item 400).

4. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., Non-installation method) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). This applies to claims 1 and 6.

5. Applicant had further argued on pages 9 – 11 that in claim 8 Parenty fails to teach the limitation that the encryption execution module fails to be downloaded in a non-installed method. Examiner respectfully disagrees. Parenty teaches the sending on an encryption execution module (Parenty, Fig. 2 Item 400, Java encryption applet).

Applicant argues that the module is not installed to the client. However, claim 8 only recites downloading a public key and an encryption execution module in a non-installed manner. Per definition, a Java applet according to a Java textbook, is defined to be any code that does not reside on the local system and must be downloaded to be run. Parenty's interpretation of the word installation maybe stated but is misleading since Java Applets are not installed by definition. Java applets are any code that does not reside on the local system but is downloaded to be run. This is also called a Java application. Evidence of this is provided in the attached Java Book.

6. Applicant's arguments in regards to 35 U.S.C.112 rejections have been considered and are deemed persuasive. The claim 35 U.S.C. 112 rejections have been withdrawn from this action.

Claim Objections

7. Claim 1 is objected to because of the following informalities: As per claim 1, on line 4 there should be an 'and' between the words 'public key' and 'a private encryption.' On line 16 the word 'form' should be 'from.' Appropriate correction is required.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 1 and 6 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

10. As per claims 1 and 6, it is indefinite as to the meaning of the phrase "driving an encryption module for encryption information to an access request from the client terminal," it will be assumed for this action to be driving and encryption module in response to an access request from a client. Also, the phrase 'double security' is indefinite to Examiner as read from the claims. It will be interpreted to be a way of emphasizing the increase in security to the system.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 1 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Parenty U.S. Publication No. (2002/0071562) in view of Cravo de Almeida et al. U.S.

Publication No. (2002/0169871), Golchikov U.S. PG-Publication No. (2002/0112158) and Hashiguchi U.S. Patent No. (6,615,353).

13. As per claims 1 and 6, Parenty discloses generating, at the server, public key, a private encryption key by driving an encryption module for encryption information to an access request from the client terminal (Parenty, Paragraph 0010), sending, at the server, to the client terminal the public key and an encryption execution module in a web document for user input in the form of a Java applet (Parenty, Paragraph 0010), sending, at the client terminal, to the server an encryption message (Parenty, Paragraph 0010) and upon receipt of the encryption message from the client terminal, decrypting, at the server, the encryption compression key by calling the private encryption key (Parenty, Paragraph 0011), but Parenty fails to disclose including a message digest module for an integrity verification and a data compression module for reduction of transmission data, and a result of compressing an original message generated by encrypting information entered from a client through the encryption execution module sent form the server and a digest message digesting the original message, and including an encryption compression key encrypted with the public key and decompressing the compressed result with the decrypted encryption compression key and decrypting the original message with the private encryption key according to a result of the integrity verification. However, Hashiguchi teaches including a message digest module for an integrity verification (Hashiguchi, Col. 4 Lines 25 - 29) and a digest message digesting the original message (Hashiguchi, Col. 4 Lines 30 - 45).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Hashiguchi's User authentication system with Parenty's system for encrypting documents for transit and storage because it offers the advantage of reliable security at a low cost (Hashiguchi, Col. 1 Lines 56 – 60).

Cravo de Almeida teaches sending a data compression module for reduction of transmission data (Cravo, Paragraph 0032).

At the time the invention was made, it would have been obvious to person of ordinary skill in the art to use Cravo de Almeida's remote monitoring with Parenty's system for encrypting documents for transit and storage because it offers the advantage of monitoring the performance of a machine which is used to understand how the processor is working (Cravo, Paragraphs 0005 – 0006).

Golchikov, teaches including a result of compressing an original message generated by encrypting information entered from a client through the encryption execution module sent form the server and decompressing the compressed result with the decrypted encryption compression key and decrypting the original message with the private encryption key according to a result of the integrity verification (Golchikov, Paragraphs 0004 and 009).

At the time the invention was made, it would have been obvious to person of ordinary skill in the art to use Golchikov's executable file protection with Parenty's system for encrypting documents for transit and storage because it offers the advantage of protecting executable files from being copied or patched (Golchikov, Paragraph 0001).

14. Claims 2, 3, 4 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Parenty U.S. Publication No. (2002/0071562), Cravo de Almeida et al. U.S. Publication No. (2002/0169871), Golchikov U.S. PG-Publication No. (2002/0112158) and Hashiguchi U.S. Patent No. (6,615,353), as applied to claim 1, and in further view of Davis et al. U.S. Patent No. (6,038,549).

15. As per claim 2, Parenty in combination with Cravo de Almeida, Golchikov and Hashiguchi, fail to disclose comparing at the server, the decrypted user authentication information with a previously stored user information database and allowing or denying, at the server, access to the client terminal to the server according to a result of information authentication. However, Davis teaches comparing at the server, the decrypted user authentication information with a previously stored user information database (Davis, Fig. 22, item 2202) and allowing or denying, at the server, access to the client terminal to the server according to a result of information authentication (Davis, Col. 29 Lines 9 – 13).

At the time the invention was made it would have been obvious to a person of ordinary skill in the art to use user authentication with Parenty's system for encrypting documents for transit and storage because it offers the advantage of securing information without exposing the content or meaning of the message (Davis, Col. 1 Lines 59 – 61, secure messaging).

16. As per claim 3, Parenty in combination with Cravo de Almeida, Golchikov and Hashiguchi, fail to disclose sending at the server, the decrypted payment information to

a financial payment institution server connected through a dedicated network and receiving, at the server, payment approval result information from the financial payment institution server and sending the received payment approval result information to the client terminal. However, Davis teaches sending at the server, the decrypted payment information to a financial payment institution server connected through a dedicated network and receiving, at the server, payment approval result information from the financial payment institution server and sending the received payment approval result information to the client terminal (Davis, Col. 13 Lines 9 – 29).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Davis' financial transaction method, with Parenty's system for encrypting documents for transit and storage because it offers the advantage of being able to perform business transactions. (Davis, Col. 1 Lines 25 – 29).

17. As per claim 4, Parenty in combination with Cravo de Almeida, Golchikov and Hashiguchi, fails to disclose public key is generated by calculating coordinates of a point on an elliptic curve with a private encryption key value of n bits generated randomly by driving the encryption and an elliptic curve initialization value. However, Davis teaches public key is generated by calculating coordinates of a point on an elliptic curve with a private encryption key value of n bits generated randomly by driving the encryption and an elliptic curve initialization value (Davis, Col. 2 Lines 64 – 67 and Col. 16 Lines 1 - 10).

18. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Davis' financial transaction method, with Parenty's system

for encrypting documents for transit and storage because it offers the advantage of being able to perform business transactions. (Davis, Col. 1 Lines 25 – 29).

19. As per claim 6, Parenty discloses generating, at the server, public key, a private encryption key by driving an encryption module for encryption information to an access request from the client terminal (Parenty, Paragraph 0010), sending, at the server, to the client terminal the public key and an encryption execution module in a web document for user input in the form of a Java applet (Parenty, Paragraph 0010), sending, at the client terminal, to the server an encryption message (Parenty, Paragraph 0010) and upon receipt of the encryption message from the client terminal, decrypting, at the server, the encryption compression key by calling the private encryption key (Parenty, Paragraph 0011), but Parenty fails to disclose including a message digest module for an integrity verification and a data compression module for reduction of transmission data and a double security by being included, including a result of compressing an original message generated by encrypting information entered from a client through the encryption execution module sent form the server and a digest message digesting the original message, and including an encryption compression key encrypted with the public key and decompressing the compressed result with the decrypted encryption compression key, decrypting the original message with the private encryption key according to a result of the integrity verification and the use of wireless terminals. However, Hashiguchi teaches including a message digest module for an

integrity verification (Hashiguchi, Col. 4 Lines 25 - 29) and a digest message digesting the original message (Hashiguchi, Col. 4 Lines 30 - 45).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Hashiguchi's User authentication system with Parenty's system for encrypting documents for transit and storage because it offers the advantage of reliable security at a low cost (Hashiguchi, Col. 1 Lines 56 – 60).

Cravo de Almeida teaches sending a data compression module for reduction of transmission data (Cravo, Paragraph 0032).

At the time the invention was made, it would have been obvious to person of ordinary skill in the art to use Cravo de Almeida's remote monitoring with Parenty's system for encrypting documents for transit and storage because it offers the advantage of monitoring the performance of a machine which is used to understand how the processor is working (Cravo, Paragraphs 0005 – 0006).

Golchikov, teaches including a result of compressing an original message generated by encrypting information entered from a client through the encryption execution module sent form the server and decompressing the compressed result with the decrypted encryption compression key and decrypting the original message with the private encryption key according to a result of the integrity verification (Golchikov, Paragraphs 0004 and 009).

At the time the invention was made, it would have been obvious to person of ordinary skill in the art to use Golchikov's executable file protection with Parenty's system for encrypting documents for transit and storage because it offers the advantage

of protecting executable files from being copied or patched (Golchikov, Paragraph 0001).

Davis teaches the use of wireless terminals (Davis, Col. 3 Lines 1 – 5).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to connect to wireless terminals with Parenty's system for encrypting documents for transit and storage because it offers the advantage of keeping a person connected to information while being mobile. (Davis, Col. 1 Lines 24 – 29, increased need for mobility).

20. Claims 5 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Parenty U.S. Publication No. (2002/0071562), Cravo de Almeida et al. U.S. Publication No. (2002/0169871), Golchikov U.S. PG-Publication No. (2002/0112158), Hashiguchi U.S. Patent No. (6,615,353) and Davis et al. U.S. Patent No. (6,038,549) in further view of Downs et al. U.S. Patent No. (6,226,618).

As per claims 5 and 7, Parenty fails to disclose digesting, at server, the decompressed original message, and comparing, at the server, the digested original message with the decompressed digest message from the client terminal and, if the digested original message and the decompressed digest are the same, decrypting the decompressed original message with the private encryption key. However, Downs teaches digesting, at server, the decompressed original message (Downs, Fig. 4 Item 412, message digest), and comparing, at the server, the digested original message with the decompressed digest message from the client terminal and, if the digested original

message and the decompressed digest are the same, decrypting the decompressed original message with the private encryption key (Downs, Fig. 4 Items 412, 414 and 417, digest comparison).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Downs' method of digesting with Parenty's system for encrypting documents for transit and storage because it offers the advantage of secure delivery and control of usage of digital assets (Downs, Col. 3 Lines 4 – 6).

Conclusion

21. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Roderick Tolentino whose telephone number is (571) 272-2661. The examiner can normally be reached on 8:00am - 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques H. Louis-Jacque can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Roderick Tolentino
Examiner
Art Unit 2134

Roderick Tolentino